Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

Groups of Order $2^{m'}$ Which Contain a Relatively Large Number of Operators of Order Two.

BY G. A. MILLER.

§ 1. *Introduction*

When exactly one-half of the operators of a group are of order 2 the group is obtained by extending an abelian group of odd order by means of an operator of order 2 which transforms each operator of this abelian group into its inverse, and if a group is constructed in this manner then exactly one-half of its operators are of order 2. If more than one-half of the operators of a group are of order 2 this excess must always be a number of the form $2^a - 1$ and there is an infinite system of such groups for every positive integral value of a.*

From the fact that the number which expresses the excess of the operators of order 2 over half the order of the group is always of the form $2^a - 1$ it results directly that in a group of order $2^{m'}$ the number of operators whose orders exceed 2 is always equal to the order of the group multiplied by a number of the form $\frac{2^n - 1}{2^{n+1}}$ and there are groups in which this product gives the number of the operators whose orders exceed 2 for every positive integral value of n. The smallest relative number of operators whose order exceeds 2 in a group of order $2^{m'}$ is therefore one-fourth of the order of the group in case there is at least one such operator.

Let G be any group in which more than one-half of the operators are of order 2. When G is abelian it is evidently of type $(1, 1, 1, \cdots)$ and hence we shall assume in what follows that G is non-abelian. As more than one-half of the operators of G are of order 2 these operators generate G and hence some of the operators of order 2 contained G must be non-invariant. If we let H_1 represent the subgroup composed of all the operators of G which are commutative with one such non-invariant operator s_1 then more than one-half of the operators of H_1 must be of order 2.

If H_1 is non-abelian it contains a non-invariant operator s_2 of order 2, and we may represent by H_2 the subgroup of H_1 composed of all its operators which are commutative with s_2. The subgroup H_1 includes the central of G

---

* *Bulletin of the American Mathematical Society*, Vol. XXV (1919), p. 33).

and H_2 includes this central as well as s_1. If H_2 is non-abelian we can continue this process until we arrive at an abelian group H_m which includes the central of G and $s_1, s_2, \cdots, s_{m-1}$. The group H_m is evidently of type $1, 1, 1, \cdots$). In the article to which we referred it was proved that $m = 1$ whenever the order of G is divisible by some odd prime number but it is possible to construct groups of order $2^{m'}$ in which m exceeds any given integer.

All the operators of G can be uniquely represented in the following form

$$H_m + H_m t_2 + H_m t_3 + \cdots + H_m t_r,$$

where it may be assumed without loss of generality that each of the operators $t_2, t_3, \cdots, t_r$ is of order 2. It is known that whenever the order of G is divisible by an odd prime number then exactly one-half of the operators in each of the co-sets $H_m t_a$, $2 \leqq a \leqq r$, are of order 2 and that in no case can more than one of these co-sets involve more operators whose orders exceed 2 than operators of order 2. In the following section we shall prove that when there is one such co-set and $r > 2$ then exactly one-fourth of its operators are of order two.

§ 2. *Less than one-half of the operators in one co-set are of order two*

The co-set in which less than one-half of the operators are of order 2 is characterized by the fact that it is composed of all the operators of G which are commutative with less than one-half of the operators of H_m. In particular, H_m contains an operator s_1 which transforms an operator t_1 of this co-set into its inverse and hence if H_1 is defined as above it does not include any operator of this co-set. Every operator of order 2 found in H_1 but not in H_m $r > 2$, is either commutative with t_1 or transforms t_1 into its inverse, for if the product of t_1 and this operator of order 2 has an order which exceeds 2 then this product is transformed into its inverse by s_1 and hence the said operator of order 2 and t_1 are commutative.

The operators of order 2 contained in H_1 but not in H_m must either generate H_1 or an abelian subgroup of type $(1, 1, 1, \cdots)$ and index 2 under H_1. The former of these alternatives is impossible since t_1 cannot be commutative with one-half of the operators of H_m. Otherwise one-half of the operators of the co-set containing t_1 would be of order 2. It therefore results that when $r > 2$ exactly one-fourth of the operators of H_m are commutative with t_1 and that the central of H_1 is a subgroup of index 2 under H_m. As exactly one-fourth of the operators of the co-set containing t_1 are of order 2 we have proved the following theorem. *Whenever one of the co-sets*

$H_m t_2, \cdots, H_m t_r$, $r > 2$, *contains more operators of order exceeding* 2 *than of order* 2 *then exactly one-fourth of the operators of this co-set are of order* 2.

It may be assumed without loss of generality that $H_m t_r$ is the co-set in which less than one-half of the operators are of order 2, and that H_1 is composed of the co-sets $H_m t_2, \cdots, H_m t_\delta$ in addition to H_m. When $\delta = 2$ the subgroup H_m is invariant under H_1 because it is of index 2. If $\delta > 2$ this subgroup is still invariant since it is generated by all the operators of order 2 found in H_1 and having more than two conjugates under H_1. It has therefore been proved that H_m is invariant under H_1 independently of the value of δ.

It is now easy to prove that H_m is also invariant under G. In fact, the operator s_1 could have been so selected that it would be commutative with all the operators of any one of the given co-sets except the co-set $H_m t_r$, and hence H_m is invariant under each of these co-sets. It therefore results that *whenever more than one-half of the operators in one of the co-sets* $H_m t_a$, $2 \leqq a \leqq r$ *have orders which exceed* 2 *then* H_m *is invariant under* G.

The quotient group G/H_m involves only operators of order 2 besides the identity and hence this quotient group must be abelian and of type $(1, 1, 1, \cdots)$. The operators of H_m which are commutative with t_r constitute the central of G and include the commutators of G which arise from operators in H_m. The former of the theorems involved in the last sentence results directly from the fact that these operators are also commutative with every operator in the co-sets $H_m t_a$, $2 \leqq a \leqq \delta$, while the latter is a consequence of the fact that each of the operators $t_2, \cdots, t_r$ transforms H_m into an automorphism of order 2. If the commutator of order 2 arising from t_a, $2 \leqq a \leqq r - 1$, would not be commutative with t_r then $t_a t_r$ could not transform H_m according to an automorphism of order 2.

Since all the commutators arising from operators of H_m are found in the central of G and since each of the operators $t_2, \cdots t_{r-1}$ is commutative with exactly one-half the operators of H_m it results that all the commutators with respect to H_m arising from these operators must also arise from t_r. As only three such commutators of order 2 arise from t_r it results that $\delta = 2$ and $r = 4$. The central of G may have any order of the form $2^{m''}$, $m'' > 1$ and there is evidently one and only one such group for every possible value of m''. Hence the following theorem has been established. *There is one and only one group of order* 2^a, $a > 5$, *such that one of the co-sets with respect to* H_m *involves more operators whose orders exceed* 2 *than operators of order* 2. *This group contains an abelian subgroup of index* 4 *and of type* $(1, 1, 1, \cdots)$ *and a central of index* 16. *The central quotient group is abelian and of type* $(1, 1, 1, \cdots)$, *and the commutator subgroup is of order* 4.

When $a > 6$ this group is evidently the direct product of the group of order 64 which belongs to this system and the abelian group of order 2^{a-6} and of type $(1, 1, 1, \cdots)$. In the form in which G presented itself above $m = 2$ but it is possible to select for s_1 an operator of H_m so as to make $m = 1$. If this is done the order of H_m remains the same since one of the corresponding co-sets must have less than one-half of its of order 2. When half of the operators of each co-set must be of order 2 it is clear that the order of H_m is independent of the choice of the set of operators $s_1, s_2, \cdots s_m$. Hence it results from the property of the groups just considered that *the order of H_m is an invariant of every group in which at least one-half of the operators are of order 2 and $r > 2$.*

It should also be noted that when $r > 2$ and G has a co-set, with respect to H_m, in which less than one-half the operators are of order 2 it must have such a co-set with respect to every possible H_m. Hence the possession of such a co-set is an invariant property of the group. When $r = 2$ this is clearly not the case, but when this condition is satisfied m is an invariant, being equal to unity, and H_1 is one of two groups. One of these must be of index 2 while for the other r may exceed 2.

If both of these subgroups are of index 2 exactly one-fourth of the operators of G have an order greater than 2 and G is known to be the direct product of the octic group and an abelian group of order 2^a and of type $(1, 1, 1, \cdots)$. When one of them has an index greater than 2 then each of the co-sets which arise with respect to this subgroup has exactly half of its operators of order 2 while the remaining operators of this co-set are of order 4 and have a common square. The co-set with respect to the other of these two subgroups contains more operators of order 4 than of order 2, the number of the operators of order 2 being half the order of the smaller subgroup which may be used for H_1. The least order which this subgroup can have when m' is odd is $\frac{1}{2}(m' - 1)$. When m' is even it is $\frac{1}{2}(m' - 2)$ since the commutator subgroup appears in the central of G.

In this system of groups for which r may be equal to 2 it is evident that there is an infinite number of groups in which the number of operators is equal to the order of the group multiplied by a number of the form $\frac{2^n - 1}{2^{n+1}}$, where n is an arbitrary positive integer. In fact, if one such group is found we can find an infinitude of others by forming the direct product of this group and abelian groups of order 2^a and of type $(1, 1, 1, \cdots)$, where a represents a positive integer but is not otherwise limited.

§ 3. *Exactly one-half of the operators of each co-set are of order 2 and $m > 1$*

When $m > 1$ and exactly one-half of the operators of each co-set are of order 2 it is easy to see that it is not possible that the subgroup of index 2 under H_m composed of all its operators which are commutative with each of the operators of one co-set is the same for all the different co-sets. Let t be any operator of order greater than 2 contained in G and let s_1 be any operator of H_m which is commutative with t but not contained in the central of G. Let H_1, as before, represent the subgroup composed of all the operators of G which are commutative with s_1.

The product obtained by multiplying any operator of order 2 contained in H_1 into an arbitrary operator whose order exceeds 2 in $G - H_1$ is transformed into its inverse by s_1 whenever the order of this product exceeds 2. In this case the two factors of this product must be commutative. As every operator whose order exceeds 2 in $G - H_1$ is transformed either into itself or into its inverse by every operator of order 2 in H_1 it results that all the operators of H_1 transform every operator of $G - H_1$ whose order exceeds 2 either into itself or into its inverse. The squares of each of the operators of H_1 is therefore contained in the central of G. In particular, t^2 is in this central. As t was any operator of order greater than 2 contained in G it results that *the squares of all the operators of G are found in the central of G and hence G involves no operator whose order exceeds* 4.

Since the quotient group of G with respect to its central involves only operators of order 2 besides the identity this quotient group must be abelian. In particular, both H_1 and H_m must be invariant subgroups of G. Every non-invariant operator of order 2 contained in G has just two conjugates. For, if such an operator s_1 had more than two conjugates, it may be supposed to appear in H_m. It may be assumed that s_1 is transformed into itself multiplied by the three distinct operators s_0, s'_0, $s_0 s'_0$ of order 2 contained in the central of G. Let t_0, t'_0, $t_0t'_0$ be three operators of G which effect these transformations respectively. If t_0 and t'_0 were not commutative with the operators of the same subgroup of index 2 under H_m there would be a co-set corresponding to H_m which would have less than half of its operators of order 2.

Hence it may be assumed that t_0 and t'_0 are commutative with the operators of the same subgroup of index 2 under G. There must be an operator t''_0 in G which is not commutative with all the operators of this subgroup. The operators of H_m which are commutative with both of the operators t_0 and t''_0 constitute a subgroup of index 4 under H_m and include the central of G. Hence t_0 and t''_0 are non-commutative with the operators of a common co-set with respect to this subgroup and it may be assumed without loss of generality that they transform the operators of this co-set into themselves multiplied by two distinct operators since t_0 may be replaced by t'_0. Hence we are again led to a co-set with respect to H_m which involves more operators whose orders exceed 2 than operators of order 2. It has therefore been proved that when $m > 1$ for every possible choice of s_1, and one-half of the operators of each co-set with respect to H_m are of order 2 then each non-invariant operator of order 2 contained in G has exactly two conjugates under G.

From the fact that each non-invariant operator of order 2 contained in G has exactly two conjugates under G it is easy to determine additional fundamental properties of G. In particular, it is possible to select a set of independent generators of G in such a way that all of these generating operators are of order 2 and that each one is commutative with all of the others with the exception of at most one of them. In fact, we may select s_1 as the first independent generator of G and then let s_2 be any operator of order two in $G - H_1$. The operators common to the two subgroups composed of all the operators of G which are commutative with s_1 and s_2 respectively constitute a subgroup of index 4 under G which includes the central of G. The order of the product of s_1 and s_2 is 4.

If this subgroup of index 4 is abelian it must be of type $(1, 1, 1, \cdots)$ and H_1 must be abelian and of the same type. In this case m would be equal to 1 and hence we may assume that the subgroup in question is non-abelian. More than one-half of its operators must be of order 2 since more than one-half of the operators of G are of order 2. It is therefore possible to find two additional non-commutative generators of order 2, s_3 and s_4, such that each of these generators is commutative with both of the operators s_1, s_2 and that $(s_3 s_4)^2 = (s_1 s_2)^2$. If the last condition were not satisfied s_1, s_3 would be an operator of order 2 having more than two conjugates under G.

When the group composed of all the operators of G which are commutative with each of the four operators s_1, s_2, s_3, s_4 is abelian and of order greater than 2 it is of type $(1, 1, 1, \cdots)$ and G is the direct product of a subgroup of index 2 under this abelian group and the group of order 32 generated by the given four operators. On the other hand, when the operators of G which are commutative with each of the four operators s_1, s_2, s_3, s_4 are not all commutative with each other then the subgroup generated by these operators must involve two non-commutative operators of order 2, s_5 and s_6, such that the square of their product is equal to $(s_1 s_2)^2$.

This process can evidently be continued until we obtain either a set of generators of G or an invariant subgroup of G of order 2^{2a+1} such that G is the direct product of this subgroup and an abelian group of type $(1, 1, 1, \cdots)$. Hence we have established the following theorem: *When m exceeds unity for every possible choice of H_m and one-half of the operators in each co-set of G with respect to H_m are of order 2 then G is generated by β operators of order 2 such that each of them is commutative with all of the others except at most one of them and the square of the product of every pair of non-commutative operators of this set is the commutator of order 2 contained in G.*

§ 4. *Exactly one-half of the operators of each co-set are of order 2 and $m = 1$*

Two cases require consideration according as $m = 1$ for every possible choice of operators from G for s_1 or as $m = 1$ for some one but not for every possible such choice. We shall first restrict our attention to the former of these cases and hence it results that the subgroup of index 2 under H_1 composed of all the operators of H_1 which are commutative with the operators of one of the $r - 1 > 1$ co-sets constitute the central of G.

Let t_1 and t_2 be two operators of order 2 found in any two distinct co-sets with respect to H_1. If t_1 and t_2 were commutative the central of G together with t_1 and t_2 would generate an abelian group of type $(1, 1, 1, \cdots)$ and of a larger order than the order of H_1. By using t_1 instead of s_1 we would therefore find a new group for H_1 which would give rise to a co-set in which less than one-half of the operators are of order 2. As this case has been considered it may be assumed that t_1 is not commutative with any operators of order 2 except those found in the central of G or in the co-set to which t_1 belongs.

Since t_1 transforms into its inverse each of the products obtained by multiplying t_1 successively into all the operators of order 2 contained in G, and as these products include all the operators of G whose orders exceed 2 it results that every operator G whose order exceeds 2 is transformed only into itself or into its inverse under G and that it must be transformed into itself by all the operators of G whose order exceeds 2 since it is transformed into its inverse by a number of operators of order 2 equal to one-half of the order of G. Hence it results that the operators whose orders exceed 2 in G generate an abelian group and that *G is either the dihedral or the extended dihedral group.*

It remains to consider the case when $r > 2$ and H_1 involves an operator s_1 which transforms every operator whose order exceeds 2 in G into its inverse and when, moreover, G contains a non-invariant operator s_2 which is commutative with operators whose orders exceed 2 in G. If the central of G is composed of half of the operators of H_1 then s_2 must be contained in an abelian group of type $(1, 1, 1, \cdots)$ whose order exceeds that of H_1. As one of the co-sets of G with respect to this abelian group would contain more operators whose orders exceed 2 than operators of order 2 it may be assumed that the order of the central of G is less than one-half of the order of H_1. It therefore results that the square of every operator of G is found in the central of G and hence H_1 is an invariant subgroup of G.

We may form H_m, $m > 1$, by starting with s_2 instead of with s_1. Let H'_2 be the subgroup of G composed of all its operators which are commutative with s_2. The product of an operator t_1 of order 4 in H'_2 and an operator t_2 of order 4 in $G - H'_2$ is transformed into its inverse by each of the operators s_1 and s_2 whenever the order of this product exceeds 2. In this case, it results therefore from a transformation by s_1 that $t_1^{-1} t_2^{-1} = t_2^{-1} t_1^{-1}$ and hence t_1 and t_2 are commutative. On the other hand, it results from a transformation by s_2 that $t_1 t_2^{-1} = t_1^{-1} t_2^{-1}$. As the latter is impossible it follows that the product of an operator of order 4 in H'_2 and an operator of this order in $G - H'_2$ must be of order 2.

As t_2 is commutative with one-half of the operators of H_m and is transformed into its inverse by the other half it results that it is commutative with all the operators of order 2 in $H'_2 - H_m$. Since t_2 is any operator of order 4 in $G - H'_2$ all of these operators are commutative with the operators of the same subgroup of index 2 under H_m. This is contrary to the hypothesis that s_2 is commutative with t_1 but not with t_2. Hence it results that *if exactly half the operators in each co-set with respect to every possible H_m are of order 2 and $m = 1$ for one choice of s_1 it must be equal to unity for every such possible choice.* Hence the central of G is of index 2 under H_1.

§ 5. *Conclusion*

The most familiar system of groups in which at least one-half of the operators are of order 2 are the dihedral and the generalized dihedral groups and when the order of a group is divisible by an odd prime number there are no other groups which have the property that at least one-half of their operators are of order 2. When the order of G is $2^{m'}$ there are other infinite systems of groups such that the number of operators of order 2 in the group exceeds half the order of the group but in all these groups the order of each operator is a divisor of 4. The dihedral and the generalized dihedral groups may be characterized by the facts that at least one-half of their operators are of order 2, that all the operators of such a group which are commutative with an arbitrary non-invariant operator of order 2 constitute an abelian group of type $(1, 1, 1, \cdots)$ and that they do not contain an abelian group of this type which is of even order and of index 2 unless the central is of index 4 or of index 1.

One of the simplest systems of groups which are neither dihedral nor extended dihedral but have the property that more than one-half of their operators are of order 2 is obtained by extending the abelian group of order $2^{m'-1}$ and of type $(1, 1, 1, \cdots)$ by means of an operator of order 2 which transforms this abelian group into itself but is commutative with less than one-half of its operators. The order of the central of such a group cannot be less than $\frac{1}{2}(m'-1)$ since the multiplying group must appear in the central. Hence these groups are possible when and only when $m' > 4$ and the number of such groups for a given value of m' is $\frac{1}{2}(m'-1)-1$ when m' is odd and $\frac{1}{2}(m'-2)-1$ when m' is even. It may be noted that for each of these groups $m=1$, but that r has two possible values.

As a second system composed of groups which are neither dihedral nor extended dihedral but have the property that more than one-half of their operators are of order 2 we may consider those for which one co-set with respect to every possible H_m has fewer operators of order 2 than of larger order. The smallest group of this system is of order 64 and every other group of the system is the direct product of this group of order 64 and an abelian group of order 2^a and of type $(1, 1, 1, \cdots)$. Exactly 7/16 of the operators of each of these groups are of order 4.

Finally, there is a third system of groups which are neither dihedral nor extended dihedral but contain more operators of order 2 than operators of larger order. This system is characterized by the facts that half of the operators in each co-set with respect to H_m are of order 2 and $m > 1$. The smallest order of such a group is 2^5 since if it is not dihedral or generalized dihedral it must contain at least two pairs of non-commutative generators when it is generated by a set of $\beta \geqq 4$ operators of order 2 such that each operator of this set is commutative with all except at most one other operator of the set. Every non-invariant operator of such a group has two conjugates under the group. By adding to the three systems just described the system composed of the dihedral and the extended dihedral groups we obtain the four possible systems of groups of order $2^{m'}$ which involve all the groups whose order is of this form and which have the property that more than one-half of their operators are of order 2.

To exhibit an important analogy between the second and the third system described above it may be desirable to note that the second system may be characterized by the fact that each of its groups may be generated by a set of

$\beta \overset{=}{>} 4$ operators of order 2 such that each of these operators is commutative with all of the others except at most one of them and that there are exactly two pairs of non-commutative operators in the set, whose products are of order 4 and have different squares. This system can also be defined by the fact that each of its groups contains the direct product of two octic groups, and when its order exceeds 64 it is the direct product of this group of order 64 and an abelian group of type $(1, 1, 1, \cdots)$.